

IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE SEARCH OF

**2504 Manor Drive
Apt. 1D
Fredericksburg , VA 22401**

Under Seal

Case No. 1:22-SW-58

IN THE MATTER OF THE SEARCH OF

**3662 Jefferson Davis Hwy
Unit 86
Fredericksburg , VA 22408**

Under Seal

Case No. 1:22-SW-59

IN THE MATTER OF THE SEARCH OF

**BLUE 2007 JEEP WRANGLER
AUTOMOBILE WITH Virginia LICENSE
PLATE ULD9457 and VIN
1J4GA59137L118552**

Under Seal

Case No. 1:22-SW-60

IN THE MATTER OF THE SEARCH OF

**BLUE 2012 HYUNDAI ELANTRA
AUTOMOBILE WITH Virginia LICENSE
PLATE WYL8162 and VIN
KMHDH4AE9CU449438**

Under Seal

Case No. 1:22-SW-61

AFFIDAVIT IN SUPPORT OF SEARCH WARRANTS

I, Jose J. Oquendo, a Special Agent with the Bureau of Alcohol, Tobacco, Firearms & Explosives (“ATF”), being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the ATF and have been so employed since 2014. I am currently assigned to the ATF Falls Church II Field Office, an enforcement group responsible for

investigating violent crime, gangs, armed drug trafficking, and other firearm related violations. In my capacity as a law enforcement officer, I have investigated individuals for the illegal possession and use of firearms.

2. I submit this affidavit in support of applications for four search warrants: (1) a search warrant for a residence located at **2504 Manor Drive, Apt. ID, Fredericksburg, VA 22401**, which is an apartment with a black door labeled “1D” listed on the door, as described in Attachment A-1; (2) a search warrant for a storage unit located at **3662 Jefferson Davis Highway, Unit 86, Fredericksburg, VA 22408**, which is a storage unit located in a storage unit facility. Unit 86 has a tan door labeled “86” listed on the door, as described in Attachment A-2; (3) a search warrant for a vehicle in the Eastern District of Virginia known as a **Blue 2007 Jeep Wrangler automobile bearing Virginia license plate number ULD9457 and vehicle identification number 1J4GA59137L118552**, which is registered to Marcus Anthony Rodriguez (“RODRIGUEZ”), as described in Attachment A-3; and a search warrant for a vehicle in the Eastern District of Virginia known as a **Blue 2012 Hyundai Elantra automobile bearing Virginia license plate number WYL8162 and vehicle identification number KMHDH4AE9CU449438**, which is registered to Rodriguez’s wife, as described in Attachment A-4.

3. Based upon the facts set forth herein, I submit there is probable cause to believe that RODRIGUEZ had knowingly manufactured machineguns in violation of federal law, sold those machineguns to persons known and unknown, and continues to engage in manufacturing and distributing machineguns in violation of federal law pursuant to violations of 18 U.S.C. § 922(o) (transfer or possess a machinegun) and 26 U.S.C. § 5861 (possession of an unregistered firearm) and that the property described in Attachments A-1, A-2, A-3, and A-4 contains

evidence, contraband, fruits, and/or instrumentalities of these criminal activities, as described, respectively, in Attachments B-1, B-2, B-3, and B-4.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show that there is probable cause for the requested warrants and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

5. On May 14, 2021, ATF received an anonymous tip through ATF's mobile app tip line, which allows users to anonymously and confidentially submit tips about crimes, regarding the sale of an AR-9 automatic rifle through Facebook. The tip named the seller of the AR-9 and showed a screenshot of a Facebook Messenger conversation between the seller who was attempting to sell the AR-9 machinegun and another individual.

6. On June 22, 2021, ATF special agents interviewed the Seller (hereafter referred to as "the Cooperating Source") in an ATF vehicle at a Target store parking lot in Fredericksburg, VA regarding the machinegun transfer. Before the interview, the Cooperating Source was advised of the Cooperating Source's *Miranda* rights. The Cooperating Source stated that the Cooperating Source understood these rights. The interview was video recorded. ATF special agents advised that the Cooperating Source was not under arrest and could leave the interview anytime. The ATF special agents asked the Cooperating Source about the Facebook Messenger chat described above, regarding the sale of an AR style machinegun. After initially denying involvement, the Cooperating Source acknowledged participating in the Facebook Messenger conversation and stated that the firearm was a machinegun. The Cooperating Source described selling the machinegun to K.A. who lives in Brandywine, Maryland for one thousand dollars.

The Cooperating Source stated that K.A. came to Fredericksburg, VA, which is in the Eastern District of Virginia, to pick up the machinegun from the Cooperating Source. The Cooperating Source described purchasing the lower receiver of the AR-9 rifle from GFR, LLC, a firearms store located in Fredericksburg, VA.

7. The Cooperating Source stated that an active-duty member of the U.S. Marine Corps named Marcus RODRIGUEZ modified the AR-9 rifle into a machinegun that was sold to K.A. The Cooperating Source stated that RODRIGUEZ has been modifying AR-style rifles into machineguns for approximately a year and a half. The Cooperating Source stated that RODRIGUEZ has a mill and a press to convert the rifles into machineguns. The Cooperating Source stated that RODRIGUEZ lives in Fredericksburg, VA. The Cooperating Source described originally meeting RODRIGUEZ through Armslist.com, a website where individuals can buy, sell, and trade firearms through private sales. The Cooperating Source stated that RODRIGUEZ charged three hundred dollars to convert the lower receiver to a fully automatic rifle. The Cooperating Source stated that RODRIGUEZ converted lower receivers without serial numbers, or “ghost lowers,” which RODRIGUEZ bought online, into machineguns. RODRIGUEZ had sent the Cooperating Source videos of RODRIGUEZ shooting the converted rifles and that the firearms function as machineguns. The Cooperating Source stated that RODRIGUEZ transported the fully automatic machineguns to Texas and sold them there. K.A. contacted the Cooperating Source through Facebook Messenger and told the Cooperating Source that the machinegun worked and that he wanted to purchase another one. The Cooperating Source contacted RODRIGUEZ and obtained an AR-15 machinegun from him which the Cooperating Source then sold to K.A.

8. On June 24, 2021, ATF conducted a search of the National Firearms Registration and Transfer Record (“NFRTR”), the central registry for all items regulated under the National Firearms Act (“NFA”), which includes machineguns, to verify if the Cooperating Source, K.A., or RODRIGUEZ had any tax stamps certifying any machinegun ownership or licenses. The search of the registry came back negative for all three and no machineguns were registered to them.

9. On July 8, 2021, ATF special agents conducted surveillance on the RODRIGUEZ residence, **2504 Manor Drive, Apt 1D, Fredericksburg, VA 22401**. The ATF special agents observed, a **blue Jeep Wrangler bearing Virginia license plate ULD9457**, parked in the apartment complex parking lot in front of the apartment building labeled 2504. A search of the National Crime Information Center (“NCIC”) revealed **the blue Jeep Wrangler bearing Virginia license plate ULD9457** is registered to RODRIGUEZ. ATF special agents observed RODRIGUEZ leave his apartment, enter **the Jeep Wrangler bearing Virginia license plate ULD9457** and depart the area. Approximately 70 minutes later, ATF special agents observed RODRIGUEZ return to the area in **the Jeep Wrangler bearing Virginia license plate ULD9457** and return to his apartment at **2504 Manor Drive, Apt 1D, Fredericksburg, VA 22401**.

10. On September 23, 2021, ATF special agents again met with the Cooperating Source. During the meeting, the Cooperating Source agreed to facilitate the purchase of a machinegun from RODRIGUEZ in furtherance of the investigation. The Cooperating Source contacted RODRIGUEZ via cell phone.

11. On September 28, 2021, an ATF special agent acting in an undercover capacity, contacted RODRIGUEZ via cell phone. Through a recorded telephone conversation and

preserved SMS/MMS messages, RODRIGUEZ agreed to sell the ATF special agent a firearm on October 1, 2021.

12. On October 1, 2021, ATF special agents conducted a controlled purchase of a firearm from RODRIGUEZ. The operation was audio and video recorded. During the operation, an ATF special agent acting in an undercover capacity purchased a custom-made Aero Precision model X15 semi-automatic rifle bearing serial number X249327 from RODRIGUEZ for \$1,900.00. RODRIGUEZ arrived at the controlled purchase location in **the Jeep Wrangler bearing Virginia license plate ULD9457**. During the transaction, RODRIGUEZ told the agent that he has manufactured machineguns in the past and has “no problem doing them.” RODRIGUEZ stated that it would take seven to ten days to receive the parts and build a machinegun. RODRIGUEZ stated that he has built firearms for other people, including firearms that he delivered to Pennsylvania and Texas. RODRIGUEZ stated that he builds the firearms in a storage unit located somewhere near his residence. RODRIGUEZ departed the purchase location in **the Jeep Wrangler**.

13. Through the recorded in-person conversation at the controlled purchase and preserved SMS/MMS messages conducted via cell phone that continued from October 1, 2021, through October 13, 2021, RODRIGUEZ agreed to manufacture an un-serialized machinegun and sell the un-serialized machinegun to the undercover agent.

14. On October 13, 2021, ATF special agents conducted a controlled purchase of an M16-type, 5.56mm NATO caliber, machinegun bearing no manufacturer’s marks or serial number from RODRIGUEZ for \$1,600.00. The transaction was audio and video recorded. RODRIGUEZ arrived at the controlled purchase location in Stafford, Virginia, in the Eastern District of Virginia, in **the blue Jeep Wrangler bearing Virginia license plate ULD9457**.

During the transaction, RODRIGUEZ provided the undercover agent with an M16-type, 5.56mm NATO caliber, machinegun, bearing no manufacturer's marks and no serial number. RODRIGUEZ explained the operation of the firearm and stated that, "It's full auto." RODRIGUEZ stated that he had built "a few" machineguns for others. RODRIGUEZ stated that he had built two others at the same time that he built the machinegun for the undercover agent and that he had two other "builds" to complete for other people. ATF special agents followed RODRIGUEZ away from the controlled purchase location, but discontinued surveillance when RODRIGUEZ entered Marine Corps Base Quantico.

15. Following the undercover controlled purchase, the firearm was function checked by ATF special agents. The firearm function checked as a machinegun.

16. On October 22, 2021, ATF agents submitted the suspected machinegun to the ATF Firearms Technology Criminal Branch for examination. On October 27, 2021, the ATF Firearms Technology Criminal Branch issued a Report of Examination regarding the firearm purchased from RODRIGUEZ on October 13, 2021 concluding that the M16-type, 5.56mm NATO caliber, firearm bearing no manufacturer's marks or serial number is a machinegun as defined by Title 18 United States Code, Section 921(a)(23) and Title 26 United States Code, Section 5845(b).

17. On November 5, 2021, U.S. Magistrate Judge Theresa C. Buchanan of the Eastern District of Virginia issued a tracking warrant under Case No. 12-SW-759 authorizing the installation and monitoring of a GPS tracking device on **the blue Jeep Wrangler bearing Virginia license plate ULD9457**. On November 9, 2021, ATF agents placed a vehicle tracker on **the blue Jeep Wrangler bearing Virginia license plate ULD9457**.

18. On November 11, 2021, the vehicle tracker showed that **the blue Jeep Wrangler bearing Virginia license plate ULD9457** traveled from RODRIGUEZ's residence at **2504 Manor Drive, Apt 1D, Fredericksburg, VA 22401** to a storage unit facility located at **3662 Jefferson Davis Highway, Fredericksburg, VA 22408**. RODRIGUEZ had earlier stated to the ATF undercover special agent that he manufactures the machineguns at a storage unit.

19. On November 28, 2021, the vehicle tracker again showed that **the Jeep Wrangler bearing Virginia license plate ULD9457** traveled to a storage unit facility located at **3662 Jefferson Davis Highway**. Law enforcement surveillance visually confirmed RODRIGUEZ was driving **the Jeep Wrangler bearing Virginia license plate ULD9457** when it left the storage unit.

20. On November 29, 2021, the ATF undercover contacted RODRIGUEZ regarding his place on the wait list for the two machineguns he had ordered from RODRIGUEZ. RODRIGUEZ text messaged a picture to the ATF undercover. The picture showed a list of individuals who were on the wait list for firearms. The list was labeled "Builds" and showed that there were two individuals listed in front of the ATF undercover order and two individuals listed after.

21. On December 3, 2021, law enforcement contacted the management of the storage unit facility located at **3662 Jefferson Davis Highway** and requested to see a unit roster of the renters of the storage units. The management provided the unit roster to law enforcement and RODRIGUEZ was listed as the renter for **storage unit number 86**.

22. On December 6, 2021, law enforcement conducted surveillance at the storage unit location and observed **the Jeep Wrangler bearing Virginia license plate ULD9457** parked at

the location of **storage unit number 86**. Law enforcement heard loud grinding coming from **storage unit number 86**.

23. On December 11, 2021, the ATF undercover contacted RODRIGUEZ regarding whether RODRIGUEZ had made progress on building the machineguns. RODRIGUEZ responded, “Nope....I’m chillin on building right now.” RODRIGUEZ further stated, “ATF paid a visit to my place.” The ATF undercover responded, “What happened” and RODRIGUEZ asked “Can you talk real quick”. The ATF undercover contacted RODRIGUEZ through a voice call. The voice call was recorded and preserved as evidence. RODRIGUEZ stated that the last gun he had built, he had built for his “buddy” and that the “buddy” had requested to send RODRIGUEZ the payment through a money app. RODRIGUEZ told his friend not to say in the app that the money was for a gun. RODRIGUEZ stated that he had received a deposit to his account for \$1,800 with a message stating “for rifle” from his friend.

24. RODRIGUEZ stated that sometime later personnel from the ATF came to his residence and requested to talk to him. RODRIGUEZ stated that the ATF agents asked him what the \$1,800 transaction for a rifle was about and RODRIGUEZ stated that he had done a custom work for his friend’s rifle. RODRIGUEZ stated that the custom work for his friend’s rifle was a paint job and installation of a drop in trigger. RODRIGUEZ stated that the ATF agents then asked about the fully automatic kits that were purchased on-line and RODRIGUEZ stated that he responded to them that he did not know that they were fully automatic kits and that he was just looking for lower parts kits for rifles. RODRIGUEZ stated that the ATF agents asked if he still had the fully automatic kits and RODRIGUEZ responded yes that he still had the fully automatic kits. RODRIGUEZ stated that he asked the ATF agents if there was any way to get rid of the

parts kits and the ATF agents stated that he could turn the kits over to a Federal Firearms Licensee (“FFL”).

25. After describing these events to the ATF undercover during the voice call, RODRIGUEZ then told the ATF undercover that he was going to wait a month before he started building another rifle. RODRIGUEZ stated that he had to be careful purchasing items and that he would now only purchase items using cash and only at the gun shows. RODRIGUEZ stated that he still had the four fully automatic kits at his residence and that he had enough kits to build both of the machineguns that were ordered by the ATF undercover. RODRIGUEZ further stated that he could possibly build the rifles and make them fully automatic later. The ATF undercover stated that he thought the fully automatic parts kits were legal to purchase. RODRIGUEZ responded that yes they were legal to purchase but that the website has a warning disclaimer stating that one needs a Class 3 license from ATF to manufacture machineguns.

26. RODRIGUEZ stated that the Cooperating Source has a friend that has fully automatic kits and that he could possibly get the kits from that individual. RODRIGUEZ suggested to the ATF undercover that he could build the two rifles to sell to the ATF undercover and later convert them into machineguns. The ATF undercover stated to RODRIGUEZ that he could wait until the machineguns were ready and RODRIGUEZ stated that he would let him know.

27. On December 16, 2021, U.S. Magistrate Judge Theresa C. Buchanan of the Eastern District of Virginia issued an order extending by forty-five (45) days, from December 20, 2021, up to and including February 3, 2022, the duration of the tracking warrant under Case No. 12-SW-759.

28. On Wednesday, January 5, 2022, RODRIGUEZ contacted the ATF undercover, via SMS/MMS message, and stated, “I’m gonna get started on the builds tomorrow....thats if yall still want them”. On Friday, January 7, 2022, the ATF undercover responded in the affirmative, and RODRIGUEZ stated that he would have the machineguns done by Friday. These messages have been preserved.

29. On Friday, January 14, 2022, ATF, Naval Criminal Investigative Service, and United States Postal Inspection Service special agents and inspectors conducted a controlled purchase of two M16-type machineguns bearing no manufacturer’s marks or serial numbers from RODRIGUEZ for \$2,700.00. One of the M16-type machineguns was a 5.56 caliber and the other M16-type machinegun was a .300 Blackout caliber. The transaction was audio and video recorded. RODRIGUEZ arrived at the controlled purchase location in Stafford, Virginia, in the Eastern District of Virginia, in a **blue Hyundai Elantra bearing Virginia license plate WYL8162**. The **Hyundai Elantra** is registered to RODRIGUEZ’s wife. During the transaction, RODRIGUEZ provided the undercover agent with two firearms bearing no manufacturer’s marks and no serial number. RODRIGUEZ stated, “they’re all full autos, they’ve got the sears in them.” I know from my training and experience that “sears” refers to auto sears that are used to convert a semi-automatic rifle into a fully automatic machinegun. RODRIGUEZ stated that he had built a 9mm AR-type rifle for his son but added a “full auto kit” for himself. RODRIGUEZ stated that he had made his wife purchase a full auto lower parts kit. Law enforcement followed RODRIGUEZ away from the controlled purchase location and observed RODRIGUEZ arrive at his residence located at **2504 Manor Dr, Apt 1D, Fredericksburg, VA 22193**.

30. Following the undercover controlled purchase, ATF special agents function checked the firearms in the field. Both firearms function checked as machineguns. The firearms were then transported to the ATF Firearms Technology Criminal Branch for further examination and a certified report, which is still pending.

31. Based on my training and experience investigating individuals involved in trafficking and manufacturing firearms, individuals store firearms, financial records (including order lists), evidence of the disposition of firearm trafficking proceeds, at their residences, storage units, other premises, and vehicles to which they have access.

**USE OF CELLULAR TELEPHONES/STORAGE MEDIA BY FIREARMS
TRAFFICKERS**

32. Based on my training, experience, and participation in firearm and firearm trafficking-related investigations, and my knowledge of this case, I know that:

- a. It is common for individuals engaged in firearms trafficking to use telephonic communications, both cellular (to include voice and text messages) and hard line, to further their criminal activities by coordinating the distribution of machineguns, illegal proceeds of firearms trafficking, and other efforts of co-conspirators;
- b. Individuals engaging in the distribution of machineguns use cellular telephones and cellular telephone technology to communicate and remain in constant contact with customers;
- c. Individuals who engage in the distribution of machineguns use cellular telephones to exchange information with customers through text messaging and instant messaging in addition to direct telephone conversations. It is also common for

firearms traffickers to send photographs and videos as exchange of information with customers; and

- d. Individuals who engage in firearms trafficking frequently maintain information, personal records, photographs, and documents in an electronic format on computers and/or smart phones.

33. Based on my training and experience, I know that it is likely that **2504 Manor Dr, Apt 1D, Fredericksburg, VA 22193; 3662 Jefferson Davis Highway, Unit 86, Fredericksburg, VA 22408**; the **Jeep Wrangler bearing Virginia license plate ULD9457**; and the **blue Hyundai Elantra bearing Virginia license plate WYL8162** may contain at least one cellular phone because of the use of cellular phones in furtherance of the distribution of machine guns described above.

34. I know from my training and experience, as well as from information found in publicly available materials including those published by cellular phone providers, that some makes and models of cellular phones offer their users the ability to unlock the device via the use of a fingerprint or thumbprint (collectively, “fingerprint”) in lieu of a numeric or alphanumeric passcode or password. This feature is called Touch ID.

35. If a user enables Touch ID on a given cellular phone device, he or she can register fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device’s Touch ID sensor. In my training and experience, users of cellular phone devices that offer Touch ID often enable it because it is considered to be a more convenient way to unlock the device than by entering a numeric or alphanumeric passcode or password, as well as a more secure way to protect the device’s contents. This is particularly true when the user(s) of the device are engaged

in criminal activities and thus have a heightened concern about securing the contents of the device.

36. In some circumstances, a fingerprint cannot be used to unlock a device that has Touch ID enabled, and a passcode or password must be used instead. These circumstances include: (1) when more than 48 hours has passed since the last time the device was unlocked, and (2) when the device has not been unlocked via Touch ID in 8 hours and the passcode or password has not been entered in the last 6 days. Thus, in the event law enforcement encounters a locked cellular phone device, the opportunity to unlock the device via Touch ID exists only for a short time. Touch ID also will not work to unlock the device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; and (3) five unsuccessful attempts to unlock the device via Touch ID are made.

37. The passcode or password that would unlock the cellular phone is not known to law enforcement. Thus, it will likely be necessary to press the finger(s) of the user(s) of the cellular phone to the device's Touch ID sensor in an attempt to unlock the device for the purpose of executing the searches authorized by these warrants. Attempting to unlock the relevant cellular phone device(s) via Touch ID with the use of the fingerprints of the user(s) is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the searches authorized by these warrants.

38. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose fingerprints are among those that will unlock the device via Touch ID, and it is also possible that the person in whose possession the device is found is not actually a user of that

device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any occupant of **2504 Manor Dr, Apt 1D, Fredericksburg, VA 22193; 3662 Jefferson Davis Highway, Unit 86, Fredericksburg, VA 22408; the Jeep Wrangler bearing Virginia license plate ULD9457; and the blue Hyundai Elantra bearing Virginia license plate WYL8162**, to press their finger(s) against the Touch ID sensor of the locked cellular phone device(s) found during the search of **2504 Manor Dr, Apt 1D, Fredericksburg, VA 22193; 3662 Jefferson Davis Highway, Unit 86, Fredericksburg, VA 22408; the Jeep Wrangler bearing Virginia license plate ULD9457; and the blue Hyundai Elantra bearing Virginia license plate WYL8162** in order to attempt to identify the device's user(s) and unlock the device(s) via Touch ID.

39. Although I do not know which of a given user's 10 fingerprints is capable of unlocking a particular device, based on my training and experience, I know that it is common for a user to unlock a Touch ID-enabled cellular phone device via the fingerprints on thumbs or index fingers. In the event that law enforcement is unable to unlock the cellular phone as described above within the attempts permitted by Touch ID, this will simply result in the device requiring the entry of a password or passcode before it can be unlocked.

40. Due to the foregoing, I request that the Court authorize law enforcement to press the fingers (including thumbs) of individuals found at **2504 Manor Dr, Apt 1D, Fredericksburg, VA 22193; 3662 Jefferson Davis Highway, Unit 86, Fredericksburg, VA 22408; the Jeep Wrangler bearing Virginia license plate ULD9457; and the blue Hyundai**

Elantra bearing Virginia license plate WYL8162 to the Touch ID sensor of cellular phones for the purpose of attempting to unlock the device via Touch ID in order to search the contents as authorized by these warrants.

41. After any cellular phones are seized, law enforcement will attempt to search them. If law enforcement cannot complete the search, then agents will send the phones to government laboratory or a private company that specializes in data extraction from electronics.

TECHNICAL TERMS

42. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. *IP Address*: The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- b. *Internet*: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. *Storage medium:* A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

43. As described above and in Attachments B-1, B-2, B-3, and B-4, respectively, these applications seek permission to search for records that might be found in **2504 Manor Dr, Apt 1D, Fredericksburg, VA 22193; 3662 Jefferson Davis Highway, Unit 86, Fredericksburg, VA 22408**; **the Jeep Wrangler bearing Virginia license plate ULD9457**; and **the blue Hyundai Elantra bearing Virginia license plate WYL8162**, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrants applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

44. *Probable cause.* I submit that if a computer or storage medium is found in **2504 Manor Dr, Apt 1D, Fredericksburg, VA 22193; 3662 Jefferson Davis Highway, Unit 86, Fredericksburg, VA 22408**; **the Jeep Wrangler bearing Virginia license plate ULD9457**; or **the blue Hyundai Elantra bearing Virginia license plate WYL8162**, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little

or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

45. *Forensic evidence.* As further described in Attachments B-1, B-2, B-3, and B-4, these applications seek permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrants, but also for forensic electronic evidence that

establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in **2504 Manor Dr, Apt 1D, Fredericksburg, VA 22193; 3662 Jefferson Davis Highway, Unit 86, Fredericksburg, VA 22408; the Jeep Wrangler bearing Virginia license plate ULD9457; and the blue Hyundai Elantra bearing Virginia license plate WYL8162** because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information

stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs,

may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrants.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

46. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrants. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrants call for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the

warrants can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data in the residence, storage unit, or vehicle to be searched. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. Variety of forms of electronic media. Records sought under these warrants could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

47. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrants I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrants, and would authorize a later review of the media or information consistent with the warrants. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrants.

48. Because people share **2504 Manor Dr, Apt 1D, Fredericksburg, VA 22193;**
3662 Jefferson Davis Highway, Unit 86, Fredericksburg, VA 22408; the Jeep Wrangler

bearing Virginia license plate ULD9457; and the blue Hyundai Elantra bearing Virginia license plate WYL8162, it is possible that the residence, storage unit, and vehicles will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that it is possible that the things described in these warrants could be found on any of those computers or storage media, the warrants applied for would permit the seizure and review of those items as well.

CONCLUSION

49. Based upon the foregoing, I submit there is probable cause to believe that RODRIGUEZ had knowingly manufactured machineguns in violation of federal law, sold those machineguns to persons known and unknown, and continues to engage in manufacturing and distributing machineguns in violation of federal law pursuant to violations of 18 U.S.C. § 922(o) (transfer or possess a machinegun) and 26 U.S.C. § 5861 (possession of an unregistered firearm) and that the property described in Attachments A-1, A-2, A-3, and A-4, contains evidence, contraband, fruits, and/or instrumentalities of these criminal activities, as described in Attachments B-1, B-2, B-3, and B-4.

Respectfully submitted,



Jose Oquendo
ATF Special Agent

Subscribed and sworn to before me on January 27, 2021

The Honorable Theresa C. Buchanan
United States Magistrate Judge

ATTACHMENT A-1

Place to be searched

The property to be searched is **2504 Manor Drive, Apt. 1D, Fredericksburg, VA 22401**, in the Eastern District of Virginia. **2504 Manor Drive, Apt. 1D, Fredericksburg, VA 22401** is an apartment with a black door labeled 1D. The apartment is located on the first floor and has a sliding rear glass door. The apartment is located within the apartment building with the numbers 2504 listed on the front of the building.



ATTACHMENT B-1

Items to be Seized

All items constituting evidence and/or instrumentalities of violations of 18 U.S.C. § 922(o) (transfer or possess a machinegun) and 26 U.S.C. § 5861 (possession of an unregistered firearm), including, but not limited to, the following:

- a. Firearms, including, but not limited to, firearms parts, accessories, holsters, and ammunition
- b. U.S. currency and other illicit gains from the distribution of firearms;
- c. Books, records, receipts, notes, ledgers, and other papers including any computerized or electronic records including cellular telephones, relating to the ordering, purchase or possession of firearms;
- d. Address and/or telephone books and papers, including computerized or electronic address and/or telephone records reflecting names, addresses and/or telephone numbers;
- e. Books, records, receipts, bank statements, and records, money drafts, letters of credit, money order and cashier's checks, receipts, pass books, bank checks, safety deposit box keys and any other items evidencing the obtaining, secreting, transfer, concealment, storage and/or expenditure of money or other assets including, but not limited to, firearms and/or firearm parts;
- f. Documents and papers evidencing ownership of firearms, possession of firearms, storage and location of such assets and facilities to safely store and secure such items, such as safes, to include lock boxes, gun safes, and strong boxes;
- g. Photographs, in particular, photographs of firearms and/or firearm parts and photographs of individuals possessing firearms and/or controlled substances and photographs showing the association of individuals;
- h. Indicia of occupancy, residence, and/or ownership of the premises described herein, including, but not limited to, utility and telephone bills, cancelled envelopes, and keys;
- i. Firearm manufacturing equipment and tools i.e. drills, lathe, and grinder.

For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, “COMPUTER”):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the COMPUTER was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the COMPUTER user’s state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER’s Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

During the execution of the search of **2504 Manor Drive, Apt. 1D, Fredericksburg, VA 22401**, described in Attachment A-1, law enforcement personnel are authorized to press the fingers (including thumbs) and faces of individuals found in **2504 Manor Drive, Apt. 1D, Fredericksburg, VA 22401** to the Touch ID or Face ID sensor of cellular phones found at **2504 Manor Drive, Apt. 1D, Fredericksburg, VA 22401** for the purpose of attempting to unlock the device via Touch ID or Face ID in order to search the contents as authorized by this warrant.

ATTACHMENT A-2

Place to be searched

The property to be searched is **3662 Jefferson Davis Highway, Unit 86, Fredericksburg, VA 22408**, in the Eastern District of Virginia. **3662 Jefferson Davis Highway, Unit 86, Fredericksburg, VA 22408** is a storage unit with a tan door labeled 86. The storage unit is located within a building labeled "Q" within the storage unit facility.



ATTACHMENT B-2

Items to be Seized

All items constituting evidence and/or instrumentalities of violations of 18 U.S.C. § 922(o) (transfer or possess a machinegun) and 26 U.S.C. § 5861 (possession of an unregistered firearm), including, but not limited to, the following:

- a. Firearms, including, but not limited to, firearms parts, accessories, holsters, and ammunition
- b. U.S. currency and other illicit gains from the distribution of firearms;
- c. Books, records, receipts, notes, ledgers, and other papers including any computerized or electronic records including cellular telephones, relating to the ordering, purchase or possession of firearms;
- d. Address and/or telephone books and papers, including computerized or electronic address and/or telephone records reflecting names, addresses and/or telephone numbers;
- e. Books, records, receipts, bank statements, and records, money drafts, letters of credit, money order and cashier's checks, receipts, pass books, bank checks, safety deposit box keys and any other items evidencing the obtaining, secreting, transfer, concealment, storage and/or expenditure of money or other assets including, but not limited to, firearms and/or firearm parts;
- f. Documents and papers evidencing ownership of firearms, possession of firearms, storage and location of such assets and facilities to safely store and secure such items, such as safes, to include lock boxes, gun safes, and strong boxes;
- g. Photographs, in particular, photographs of firearms and/or firearm parts and photographs of individuals possessing firearms and/or controlled substances and photographs showing the association of individuals;
- h. Indicia of occupancy, residence, and/or ownership of the premises described herein, including, but not limited to, utility and telephone bills, cancelled envelopes, and keys;
- i. Firearm manufacturing equipment and tools i.e. drills, lathe, and grinder.

For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, “COMPUTER”):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the COMPUTER was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the COMPUTER user’s state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER’s Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

During the execution of the search of **3662 Jefferson Davis Highway, Unit 86, Fredericksburg, VA 22408**, described in Attachment A-2, law enforcement personnel are authorized to press the fingers (including thumbs) and faces of individuals found in **3662 Jefferson Davis Highway, Unit 86, Fredericksburg, VA 22408** to the Touch ID or Face ID sensor of cellular phones found at **3662 Jefferson Davis Highway, Unit 86, Fredericksburg, VA 22408** for the purpose of attempting to unlock the device via Touch ID or Face ID in order to search the contents as authorized by this warrant.

ATTACHMENT A-3

Property to be searched

The property to be searched is a **2007 Blue Jeep Wrangler** bearing Virginia license plate **ULD9457** and vehicle identification number **1J4GA59137L118552**.



ATTACHMENT B-3

Items to be Seized

All items constituting evidence and/or instrumentalities of violations of 18 U.S.C. § 922(o) (transfer or possess a machinegun) and 26 U.S.C. § 5861 (possession of an unregistered firearm), including, but not limited to, the following:

- a. Firearms, including, but not limited to, firearms parts, accessories, holsters, and ammunition
- b. U.S. currency and other illicit gains from the distribution of firearms;
- c. Books, records, receipts, notes, ledgers, and other papers including any computerized or electronic records including cellular telephones, relating to the ordering, purchase or possession of firearms;
- d. Address and/or telephone books and papers, including computerized or electronic address and/or telephone records reflecting names, addresses and/or telephone numbers;
- e. Books, records, receipts, bank statements, and records, money drafts, letters of credit, money order and cashier's checks, receipts, pass books, bank checks, safety deposit box keys and any other items evidencing the obtaining, secreting, transfer, concealment, storage and/or expenditure of money or other assets including, but not limited to, firearms and/or firearm parts;
- f. Documents and papers evidencing ownership of firearms, possession of firearms, storage and location of such assets and facilities to safely store and secure such items, such as safes, to include lock boxes, gun safes, and strong boxes;
- g. Photographs, in particular, photographs of firearms and/or firearm parts and photographs of individuals possessing firearms and/or controlled substances and photographs showing the association of individuals;
- h. Indicia of occupancy, residence, and/or ownership of the premises described herein, including, but not limited to, utility and telephone bills, cancelled envelopes, and keys;
- i. Firearm manufacturing equipment and tools i.e. drills, lathe, and grinder.

For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, “COMPUTER”):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the COMPUTER was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the COMPUTER user’s state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER’s Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

During the execution of the search of the **2007 Blue Jeep Wrangler bearing Virginia license plate ULD9457 and vehicle identification number 1J4GA59137L118552**, described in Attachment A-3, law enforcement personnel are authorized to press the fingers (including thumbs) and faces of individuals found in the **2007 Blue Jeep Wrangler bearing Virginia license plate ULD9457 and vehicle identification number 1J4GA59137L118552** to the Touch ID or Face ID sensor of cellular phones found in the **2007 Blue Jeep Wrangler bearing Virginia license plate ULD9457 and vehicle identification number 1J4GA59137L118552** for the purpose of attempting to unlock the device via Touch ID or Face ID in order to search the contents as authorized by this warrant.

ATTACHMENT A-4

Property to be searched

The property to be searched is a **2012 Blue Hyundai Elantra bearing Virginia license plate WYL8162 and vehicle identification number KMHDH4AE9CU449438.**



ATTACHMENT B-4

Items to be Seized

All items constituting evidence and/or instrumentalities of violations of 18 U.S.C. § 922(o) (transfer or possess a machinegun) and 26 U.S.C. § 5861 (possession of an unregistered firearm), including, but not limited to, the following:

- a. Firearms, including, but not limited to, firearms parts, accessories, holsters, and ammunition
- b. U.S. currency and other illicit gains from the distribution of firearms;
- c. Books, records, receipts, notes, ledgers, and other papers including any computerized or electronic records including cellular telephones, relating to the ordering, purchase or possession of firearms;
- d. Address and/or telephone books and papers, including computerized or electronic address and/or telephone records reflecting names, addresses and/or telephone numbers;
- e. Books, records, receipts, bank statements, and records, money drafts, letters of credit, money order and cashier's checks, receipts, pass books, bank checks, safety deposit box keys and any other items evidencing the obtaining, secreting, transfer, concealment, storage and/or expenditure of money or other assets including, but not limited to, firearms and/or firearm parts;
- f. Documents and papers evidencing ownership of firearms, possession of firearms, storage and location of such assets and facilities to safely store and secure such items, such as safes, to include lock boxes, gun safes, and strong boxes;
- g. Photographs, in particular, photographs of firearms and/or firearm parts and photographs of individuals possessing firearms and/or controlled substances and photographs showing the association of individuals;
- h. Indicia of occupancy, residence, and/or ownership of the premises described herein, including, but not limited to, utility and telephone bills, cancelled envelopes, and keys;
- i. Firearm manufacturing equipment and tools i.e. drills, lathe, and grinder.

For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, “COMPUTER”):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the COMPUTER was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the COMPUTER user’s state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER’s Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

During the execution of the search of the **2012 Blue Hyundai Elantra bearing Virginia license plate WYL8162 and vehicle identification number KMHDH4AE9CU449438**, described in Attachment A-4, law enforcement personnel are authorized to press the fingers (including thumbs) and faces of individuals found in the **2012 Blue Hyundai Elantra bearing Virginia license plate WYL8162 and vehicle identification number KMHDH4AE9CU449438** to the Touch ID or Face ID sensor of cellular phones found in the **2012 Blue Hyundai Elantra bearing Virginia license plate WYL8162 and vehicle identification number KMHDH4AE9CU449438** for the purpose of attempting to unlock the device via Touch ID or Face ID in order to search the contents as authorized by this warrant.